nedeljainformatike v7.0

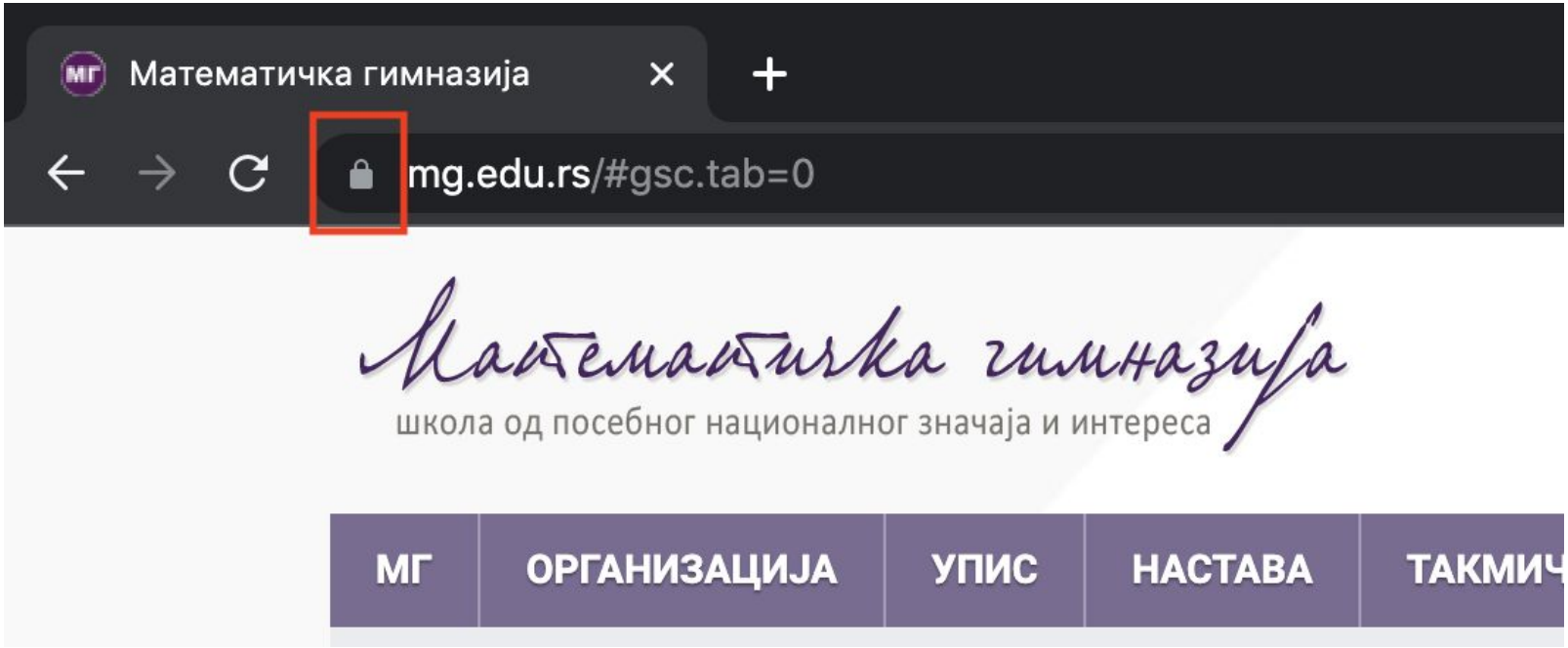
Kako da znaš da si na željenom sajtu?

Marina Ivanović

Matematička gimnazija

13. 04. 2022.

Šta znači ovaj katanac?

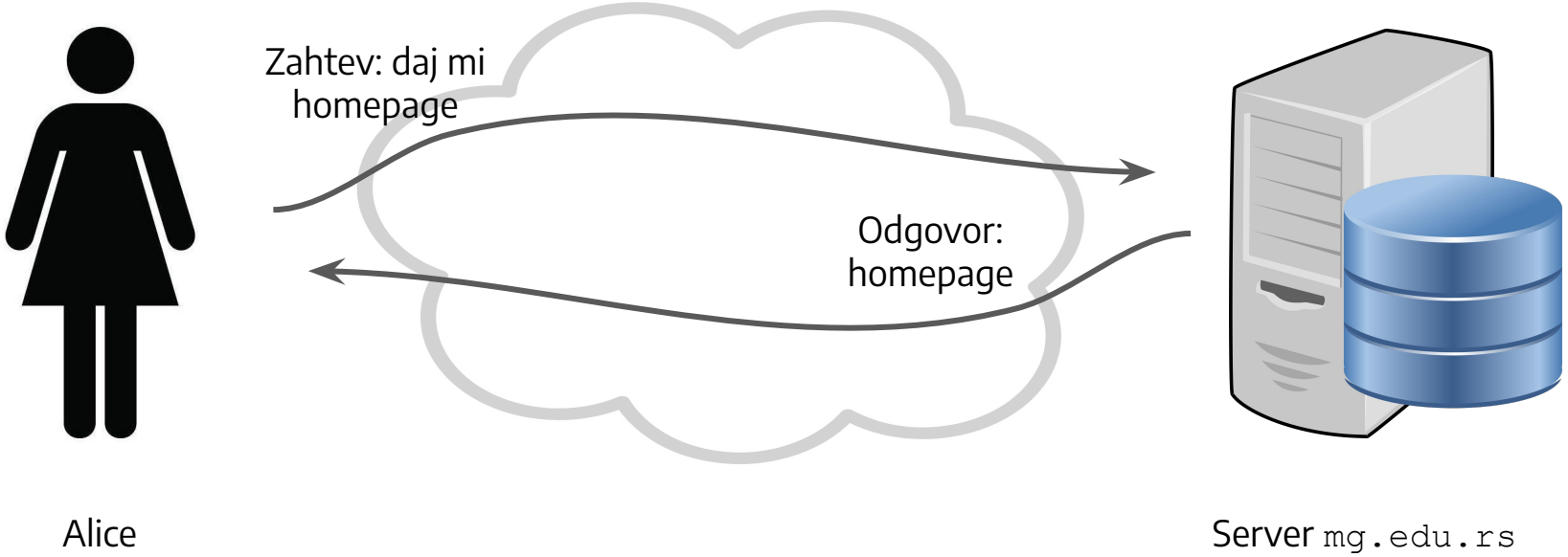


Taj katanac znači dve stvari...

1. Komunikacija između našeg browser-a i servera `mg.edu.rs` je **enkriptovana**.

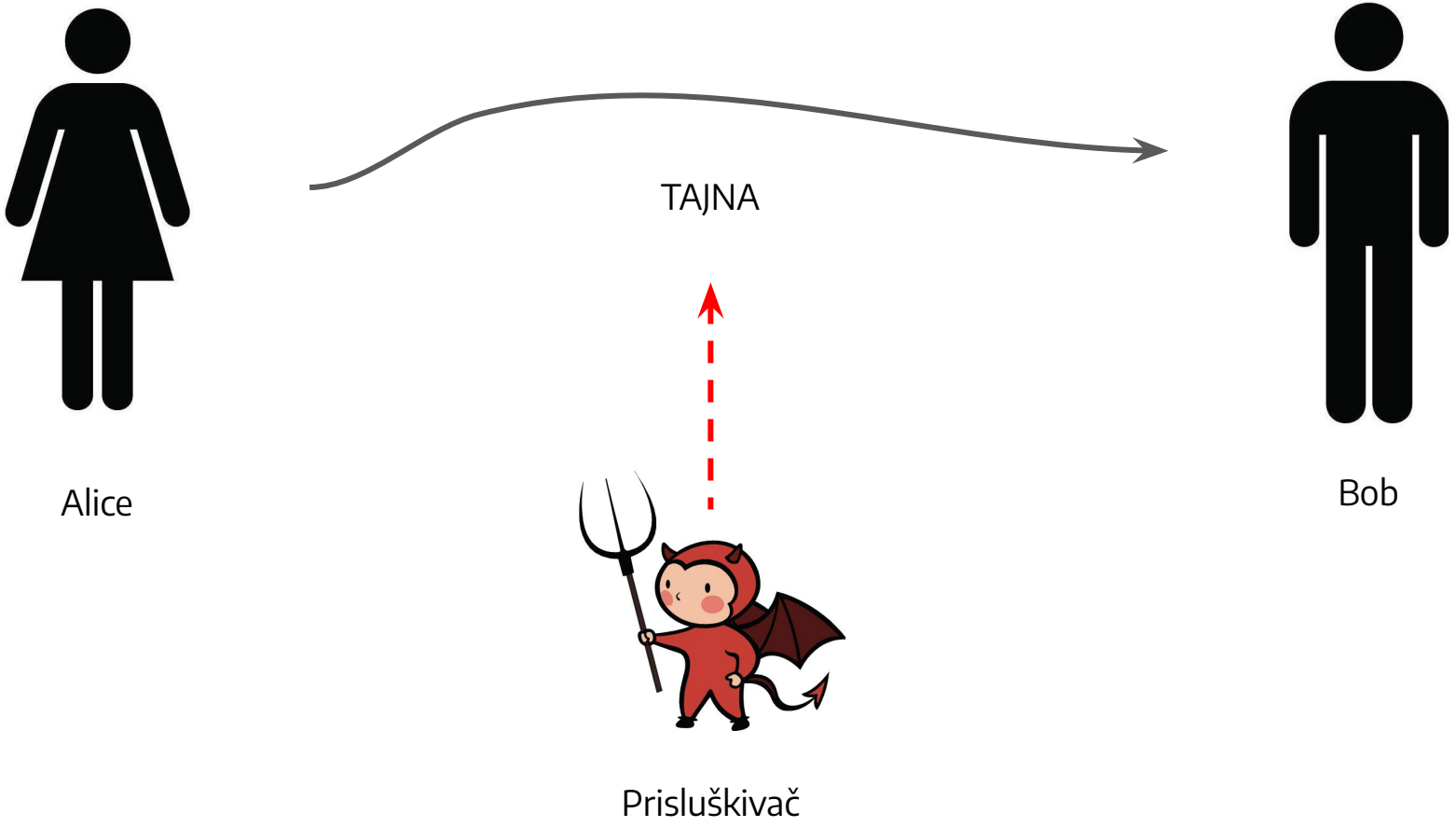
2. Server sa kojim moj browser komunicira ima “dokaz” da je on server od sajta `mg.edu.rs`. Taj “dokaz” se u digitalnom svetu zove **sertifikat**.

Komunikacija sa serverom

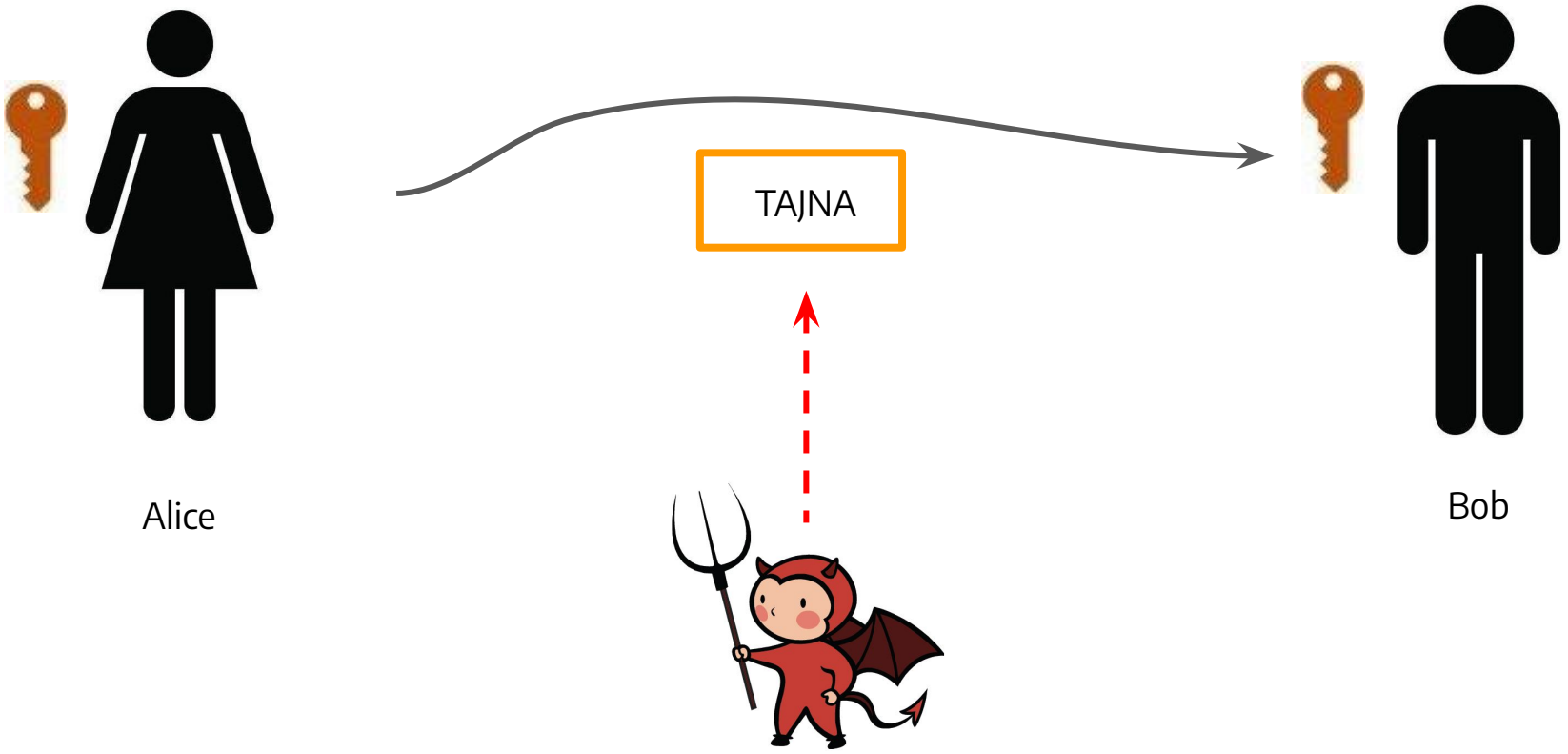


Enkripcija

Zašto nam treba enkripcija?

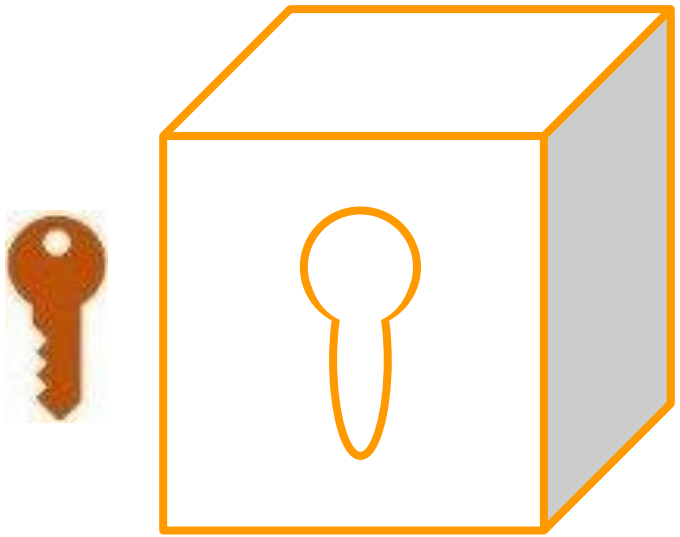


Simetrična Enkripcija

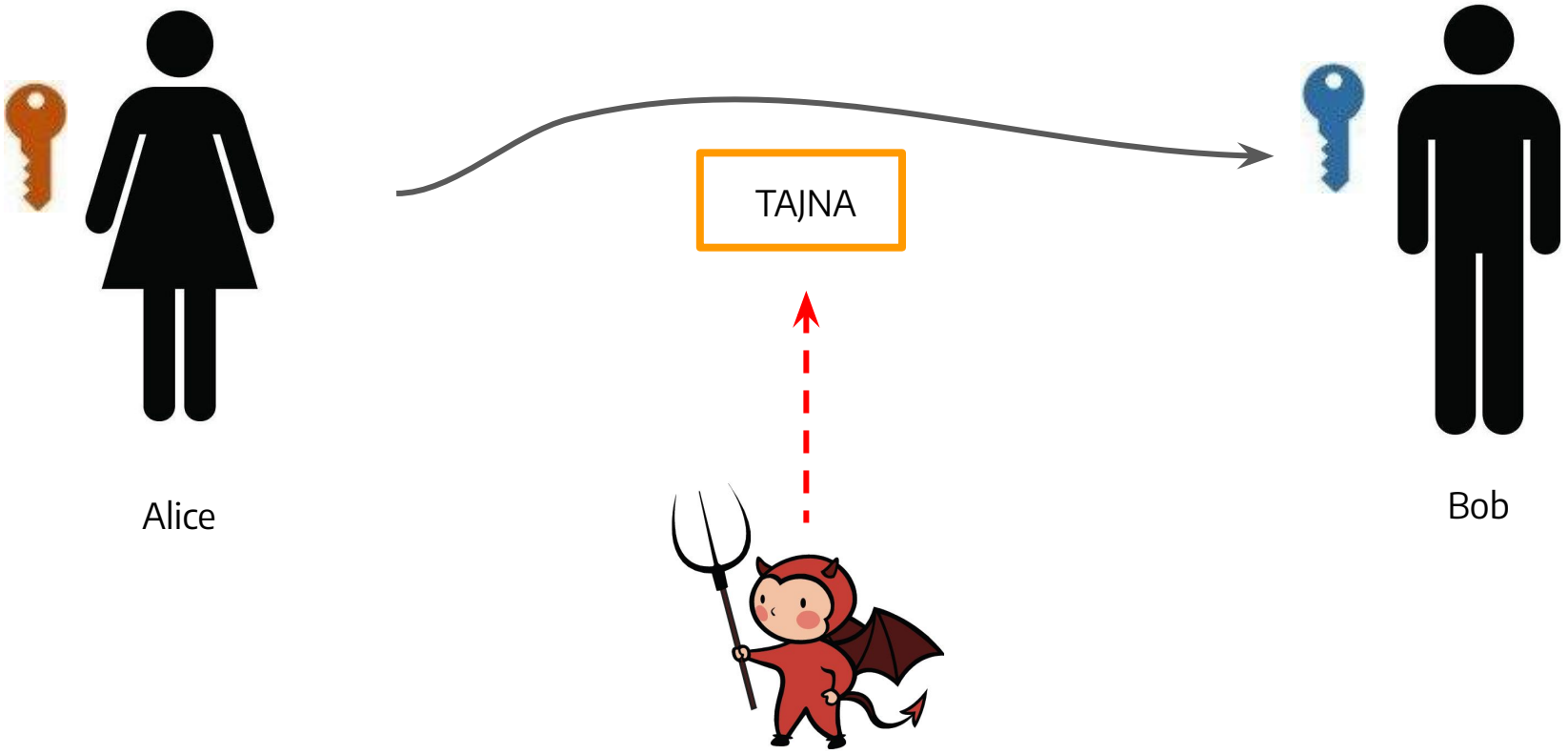


Intuicija iza simetrične enkripcije

Poruka je smeštena u “kutiju” koja se može otvoriti samo odgovarajućim **ključem**.
⇒ Poruku može videti samo onaj ko ima taj ključ, i niko drugi

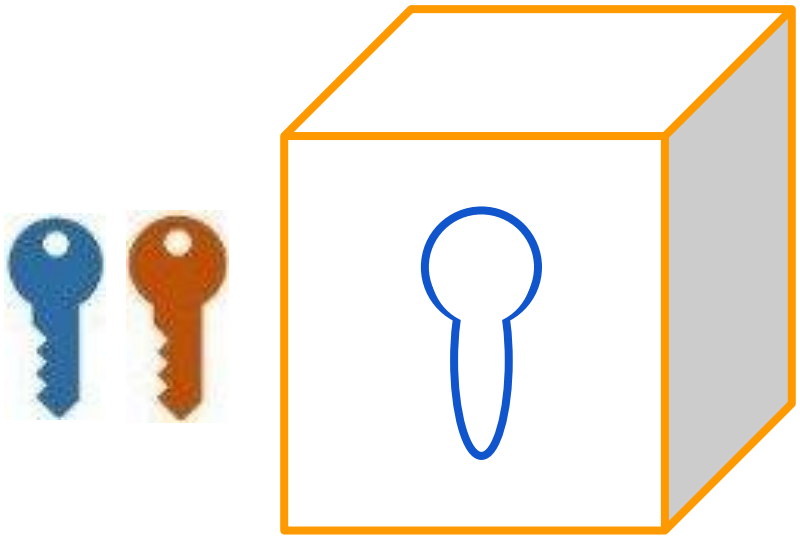


Asimetrična Enkripcija



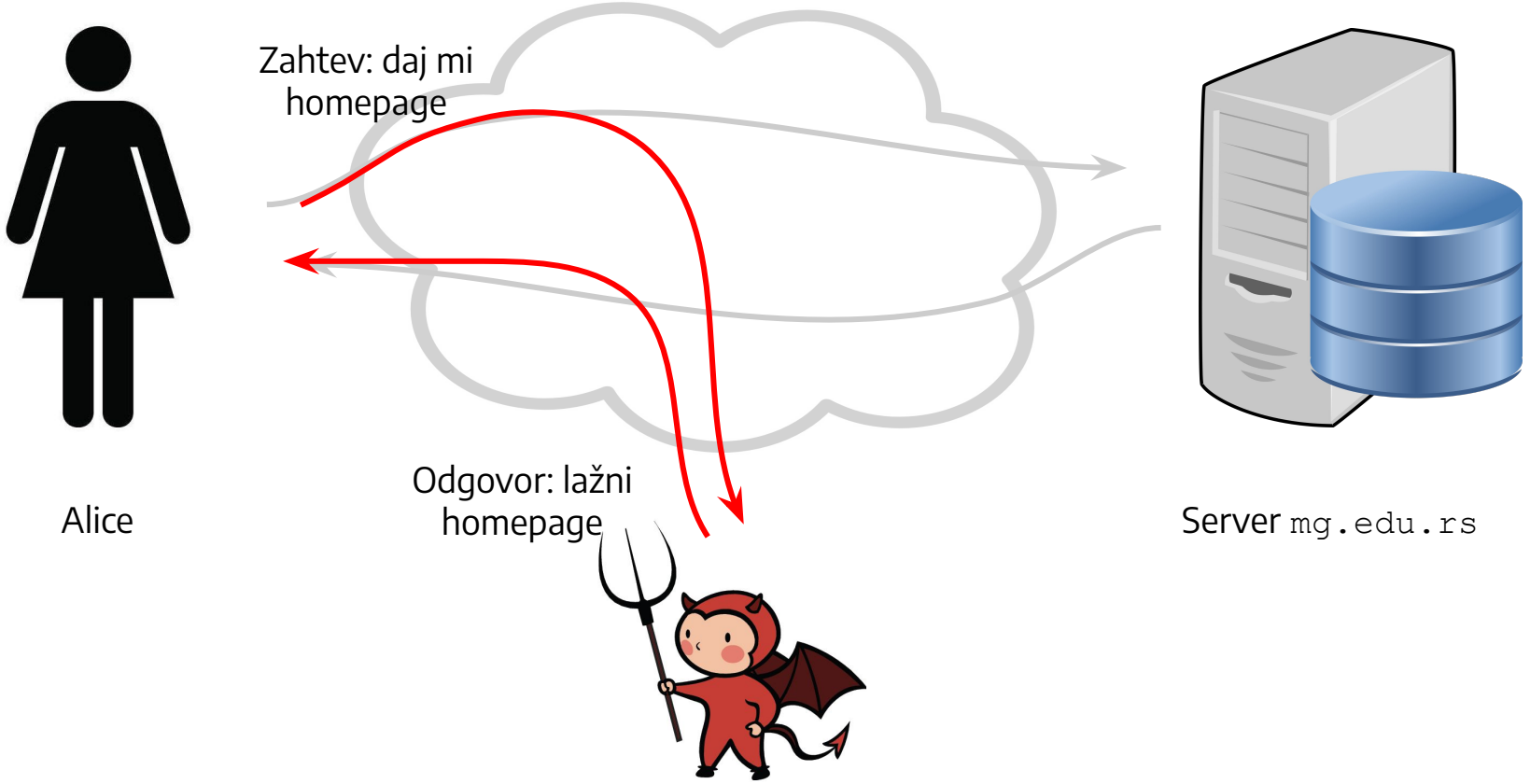
Intuicija iza asimetrične enkripcije

Poruka je smeštena u “kutiju”, i ta kutija je **javni ključ**. Kutija se “sama zaključa” kada se poruka stavi u nju ⇒ Poruku može videti samo onaj ko ima **privatni ključ**



Sertifikati

Zašto nam treba sertifikat?

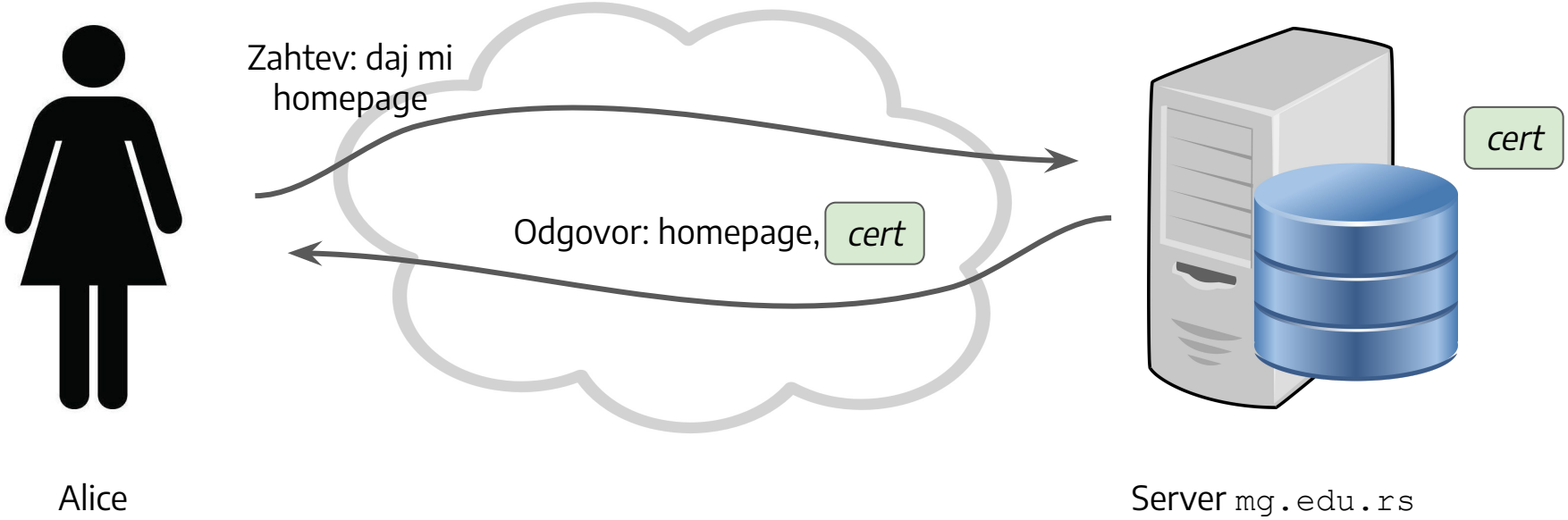


Kako da znaš da si na željenom sajtu?

Taj sajt mora ti dati dokaz da je to zaista sajt za koji se predstavlja!

U suprotnom – ne možeš znati da si na željenom sajtu. Neko je možda presreo tvoju konekciju i predstavlja se kao taj sajt, iako zapravo nije!

Server ti šalje sertifikat



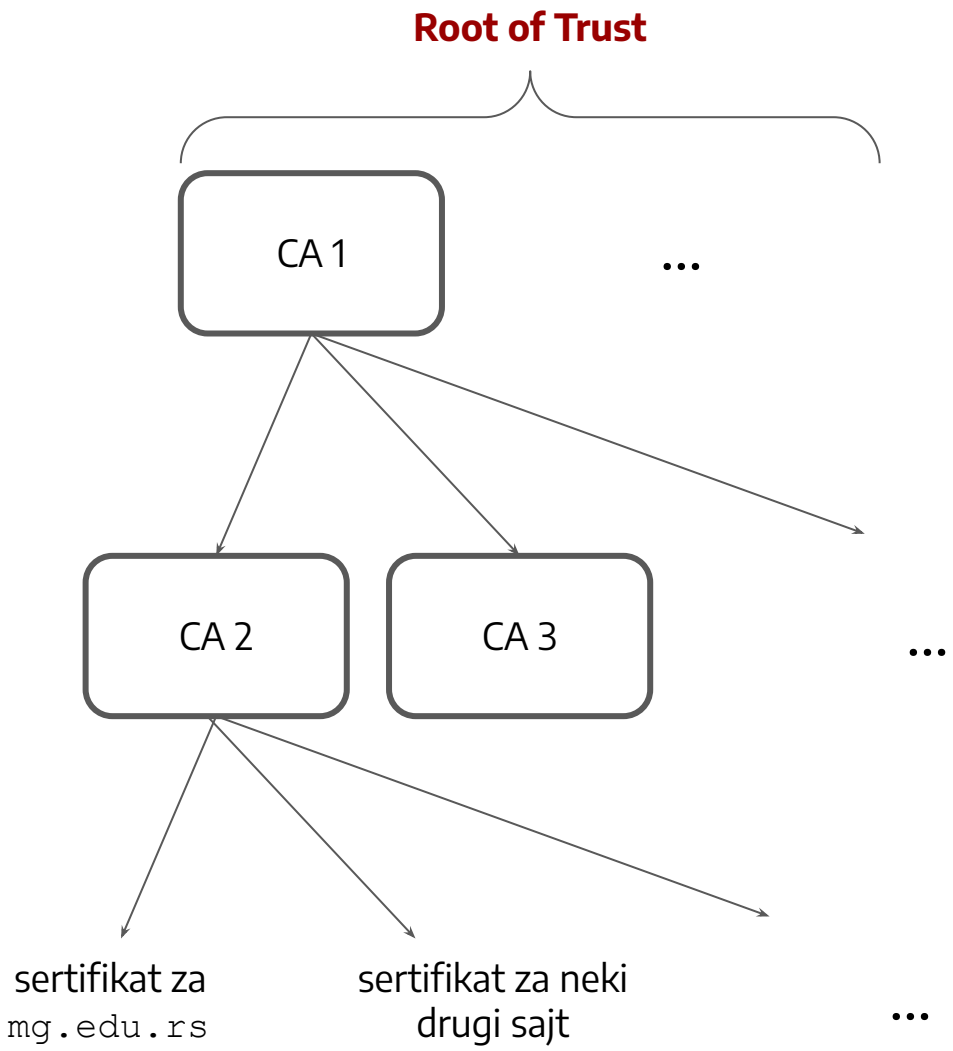
Izdavanje sertifikata

Ko garantuje da je sertifikat validan?

Svaki validan sertifikat mora biti izdat od strane validnog “certificate authority” (CA).

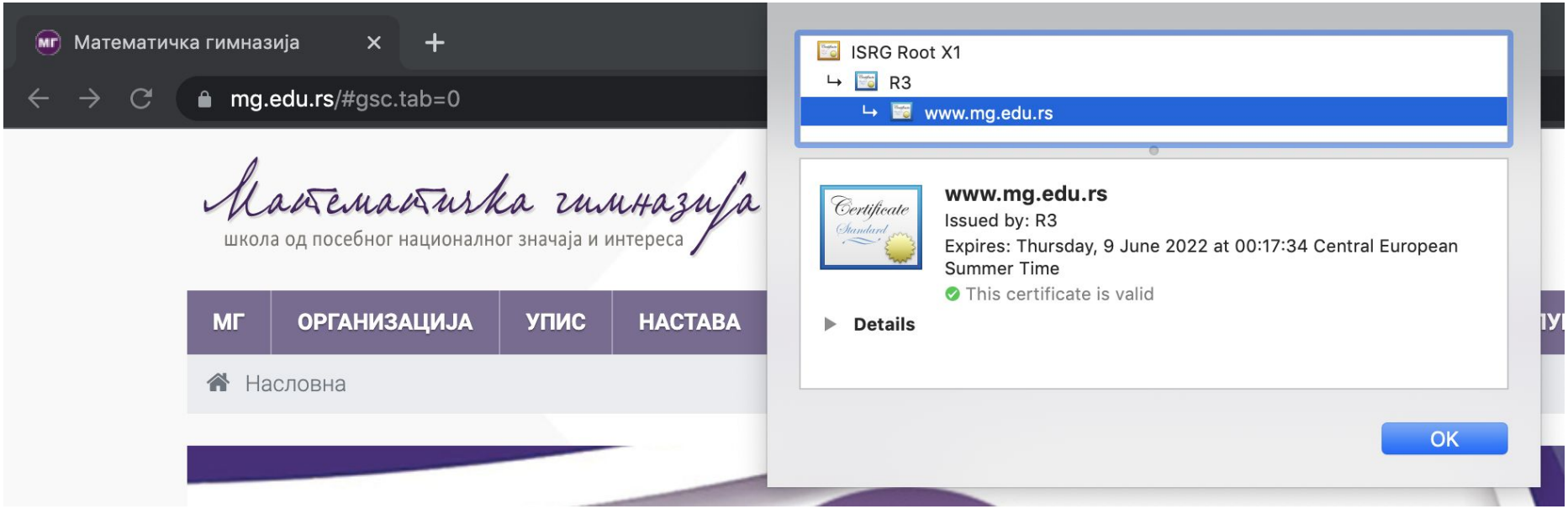
Sertifikat “ima pečat” od strane validnog CA-a koji garantuje validnost.

Certificate Authorities (CAs)

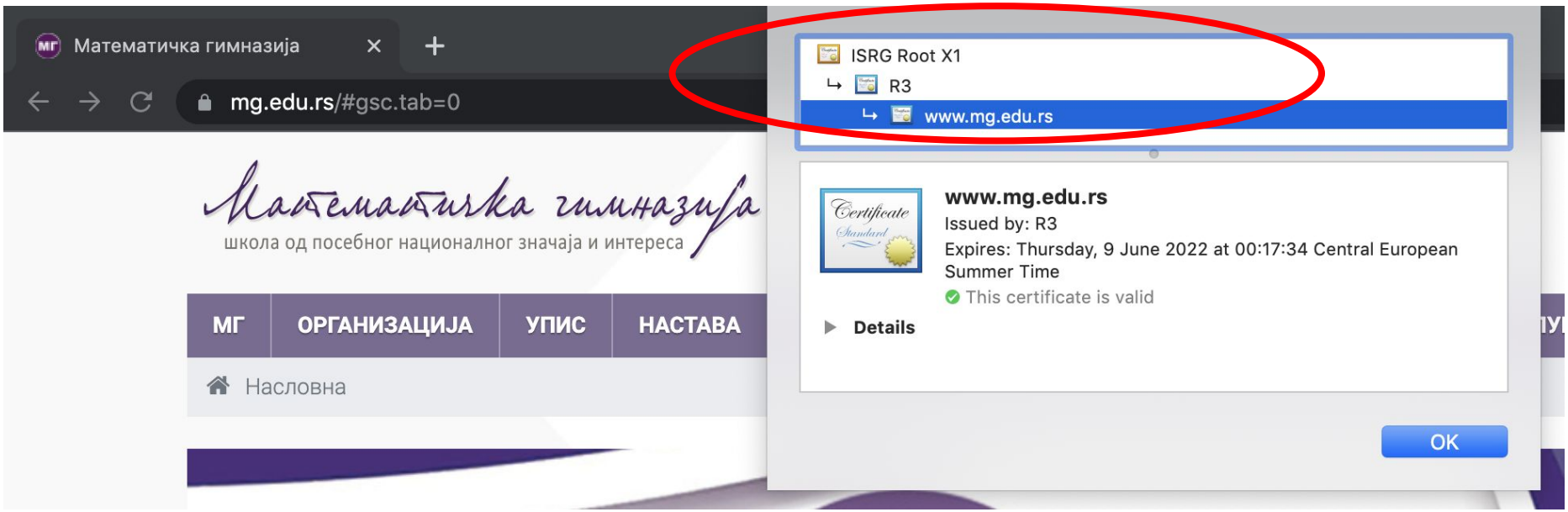


Sertifikat možeš videti u browser-u

Klik na katanac → klik na “Connection is secure” → klik na “Certificate is valid”



...kao i sve CAs koji garantuju njegovu validnost



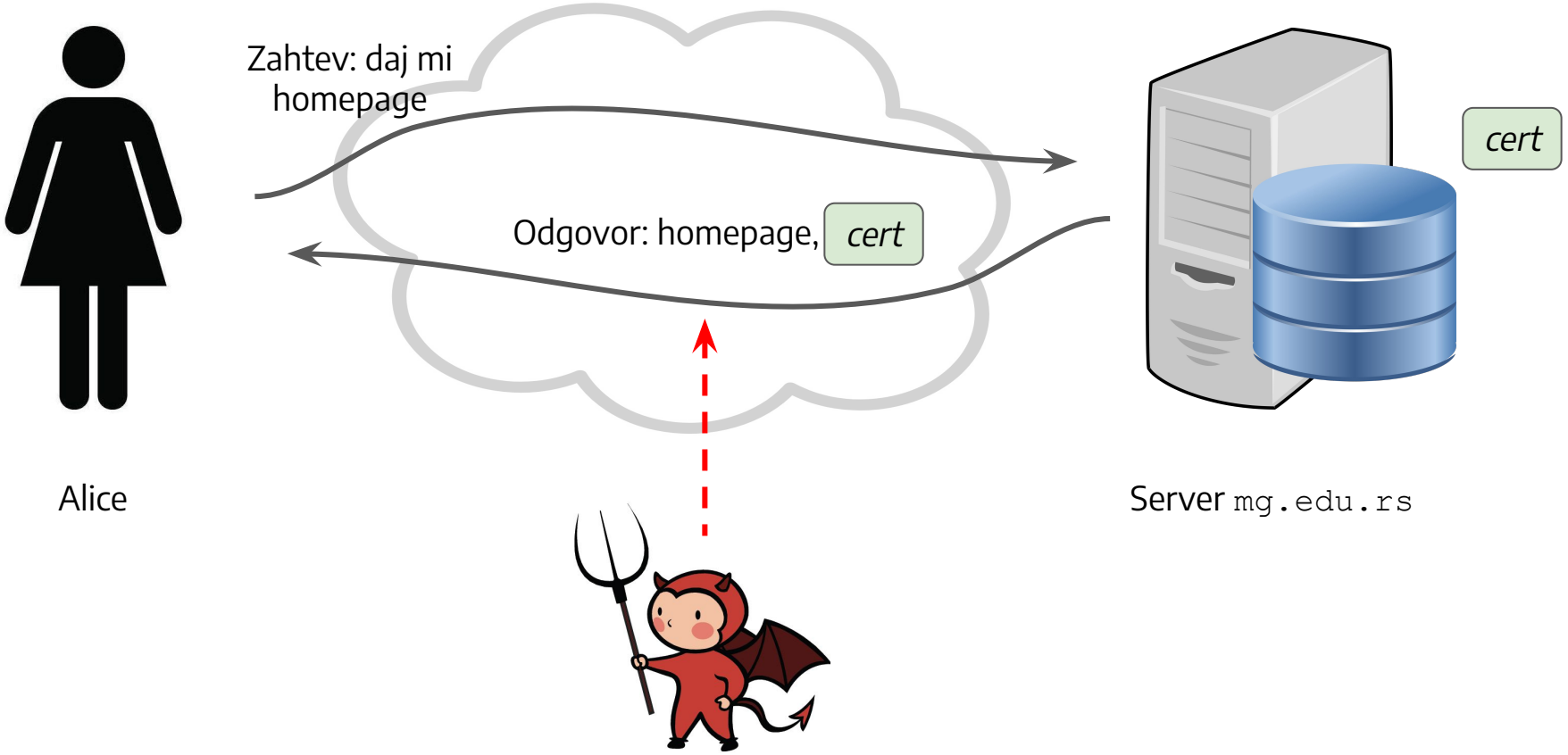
Kako moj kompjuter zna da je *cert* validan?

U tvom kompjuteru se nalazi spisak svih “roots of trust” kojima on veruje.

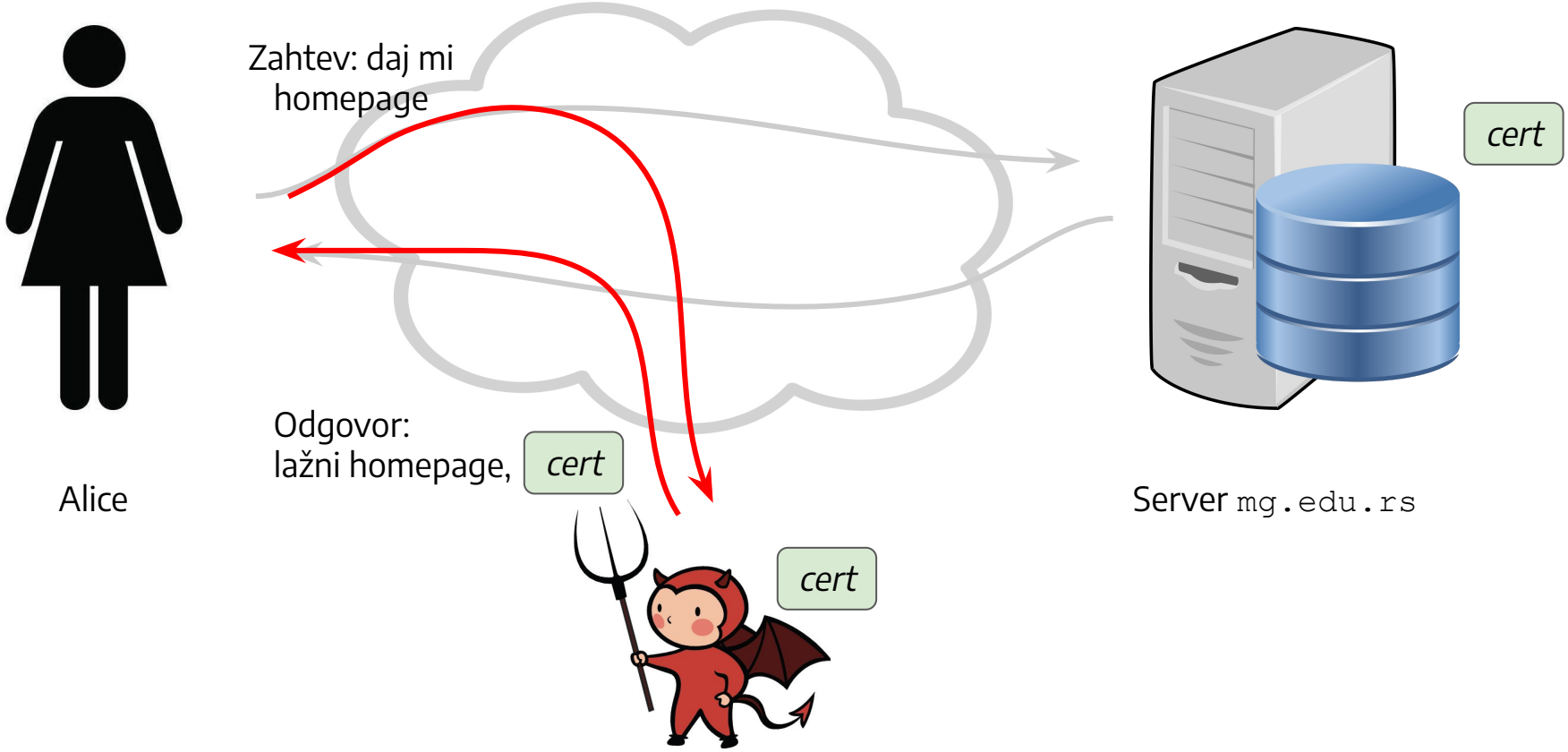
Kada dobije sertifikat, lančano prati sve CAs koji su ga potvrdili. Ako se u korenu nalazi neki od “roots of trust” kojima on veruje, to znači da je *cert* validan.

Sme li ovo da se dogodi?

Prisluškivač prisluškuje, i sačuva *cert* kod sebe



Sutradan, daje Alice *cert* da dokaže (lažan) identitet



Ovo ne sme da se dogodi!

Sertifikat mora da garantuje identitet sajta. Dakle, ako neko drugi ima samo sertifikat, to ne sme da bude dovoljno da se lažno predstavi kao taj sajt.

⇒Sertifikat garantuje da sajt sa kojim razgovaram ima nešto privatno, što ne može imati niko drugi. To “nešto privatno” je **privatni ključ**.

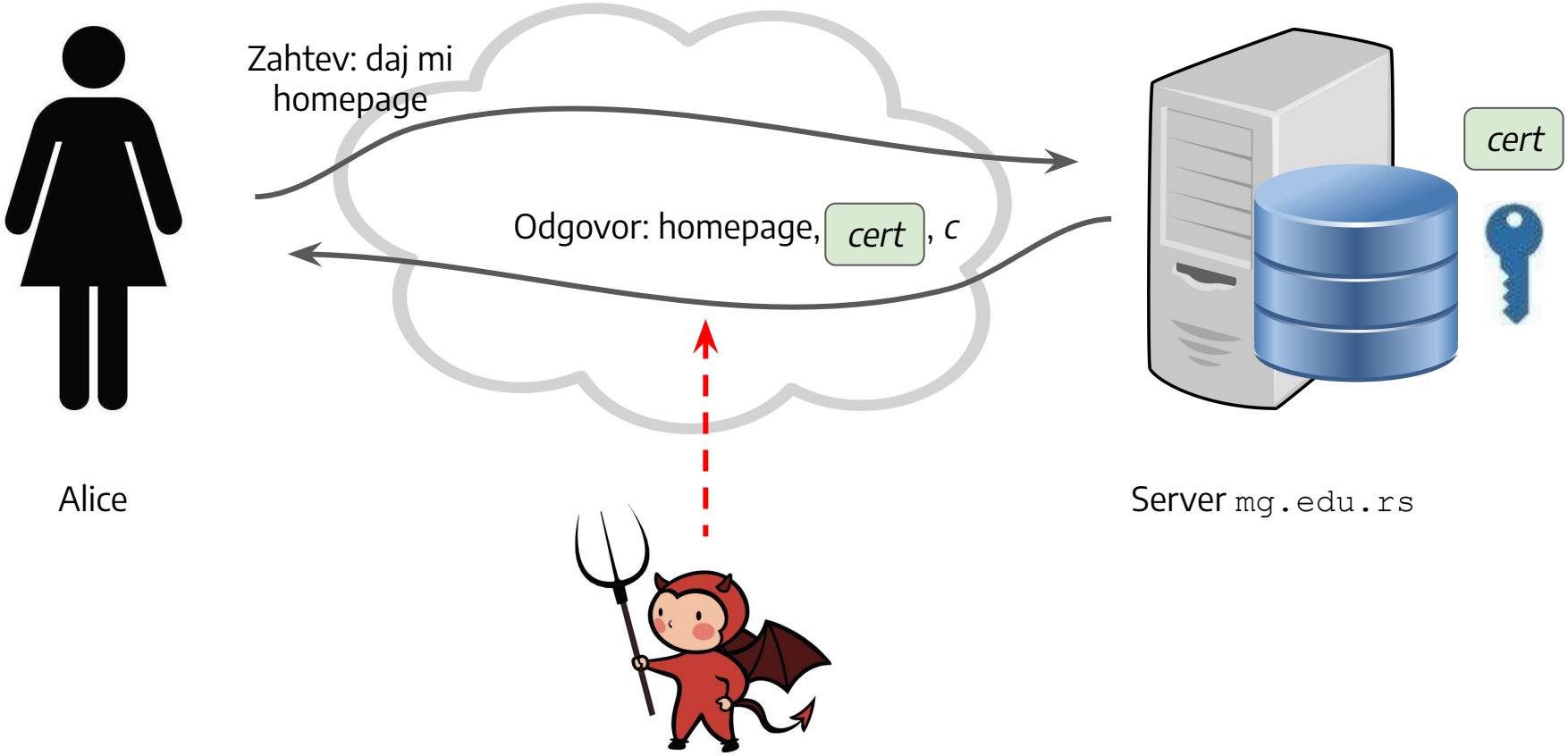
Kako izgleda sertifikat?

Sertifikat

Ovo je **javni ključ** od sajta `mg.edu.rs`: 

Ovo potvrđuje CA koji je akreditovan od strane...

Pored *cert* server šalje i neku vrednost *c*



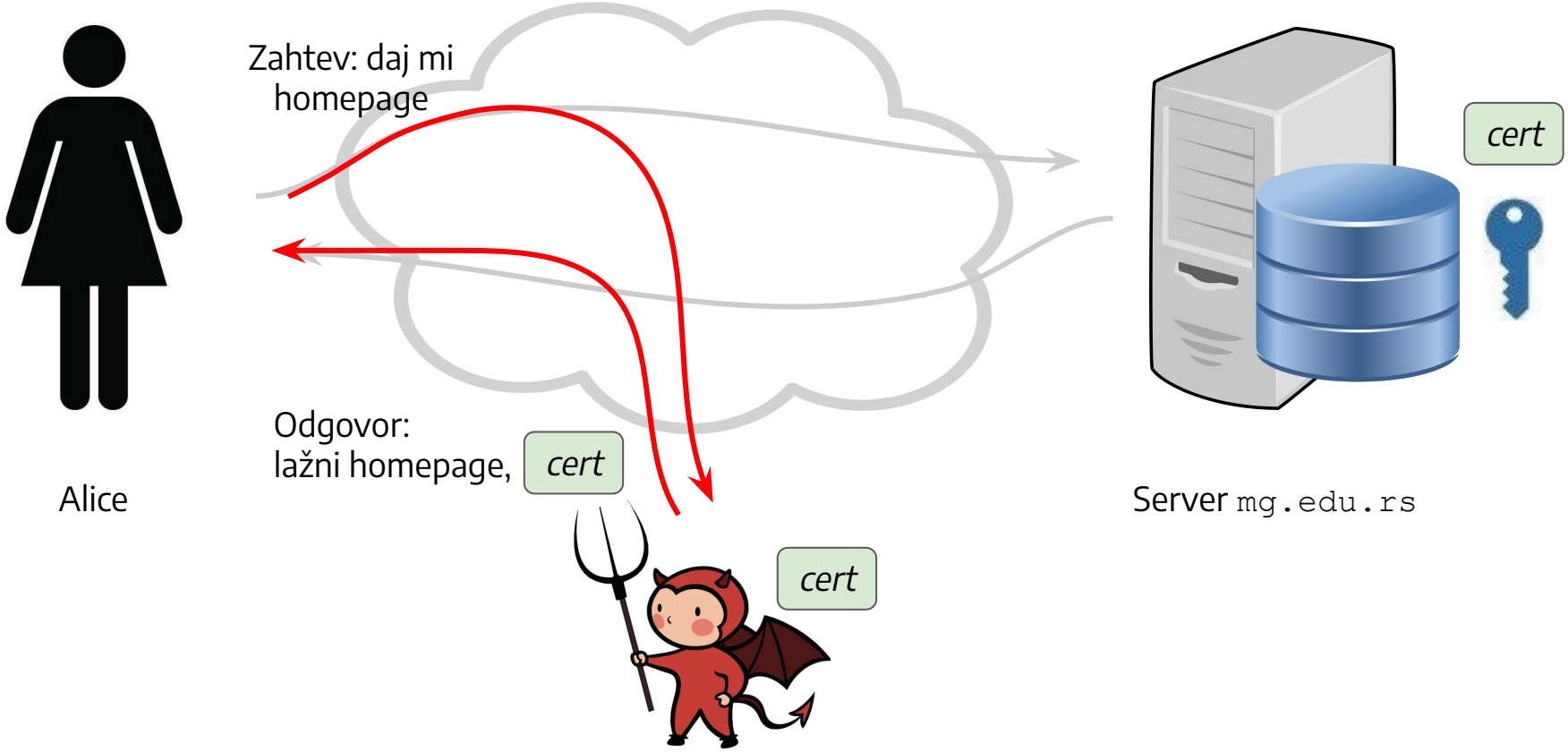
c otprilike ovako nekako izgleda

c = Encrypt_  (“ovo sam stvarno ja”)

…. kada Alice ovo dekriptuje javnim ključem koji je potvrđen sertifikatom, mora da dobije validnu poruku. Ako ne dobije validnu poruku, to znači da server ne može da potvrdi da ima odgovarajući privatni ključ.

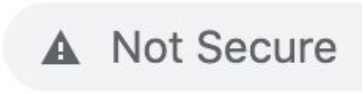
Decrypt_  (c) = “ovo sam stvarno ja”

Ovo se sada lako detektuje kao prevara



Primeri i problemi

“Connection is secure”



- HTTP - protokol u kojem nema nikakve enkripcije i sertifikata

- HTTPS - HTTP koji je Secure

⇒ NIKADA nemojte pisati nijednu šifru na sajtu koji koristi samo HTTP, ili na sajtu koji nema naznaku da je “secure”!

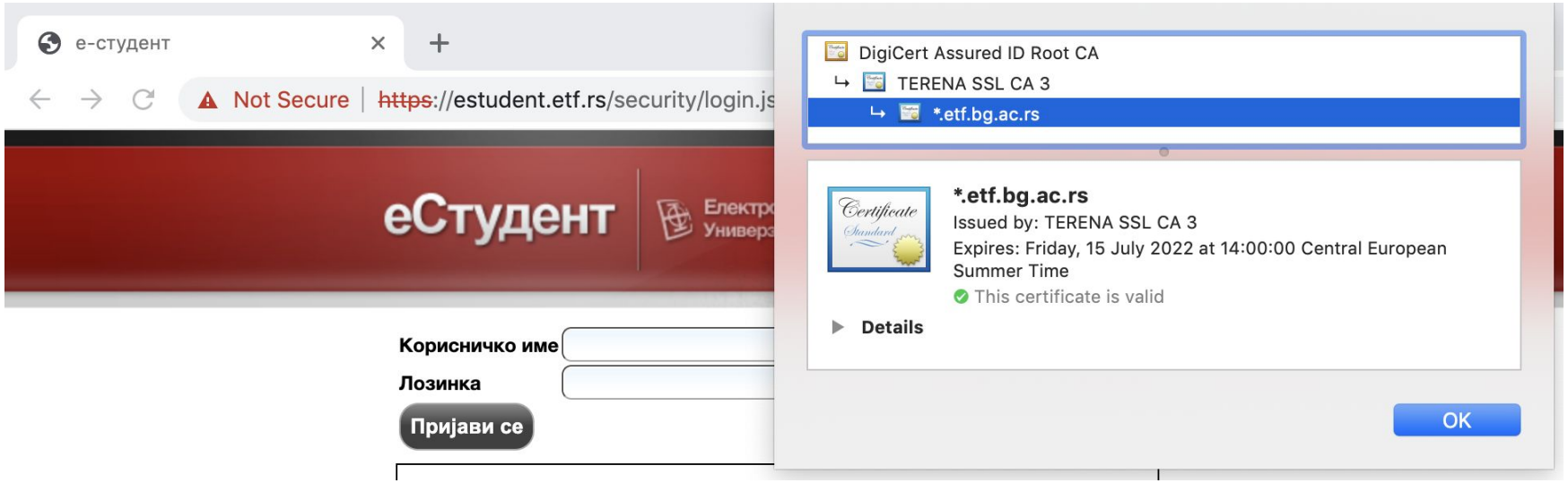
HTTPS, a ne piše “Secure”

Ovo se može desiti iz nekoliko razloga. Na primer:

1. Sajt nije priložio sertifikat koji je verifikovan od strane CA kojem verujemo.
2. Sajt nije uspeo da dokaže da poseduje odgovarajući privatni ključ.

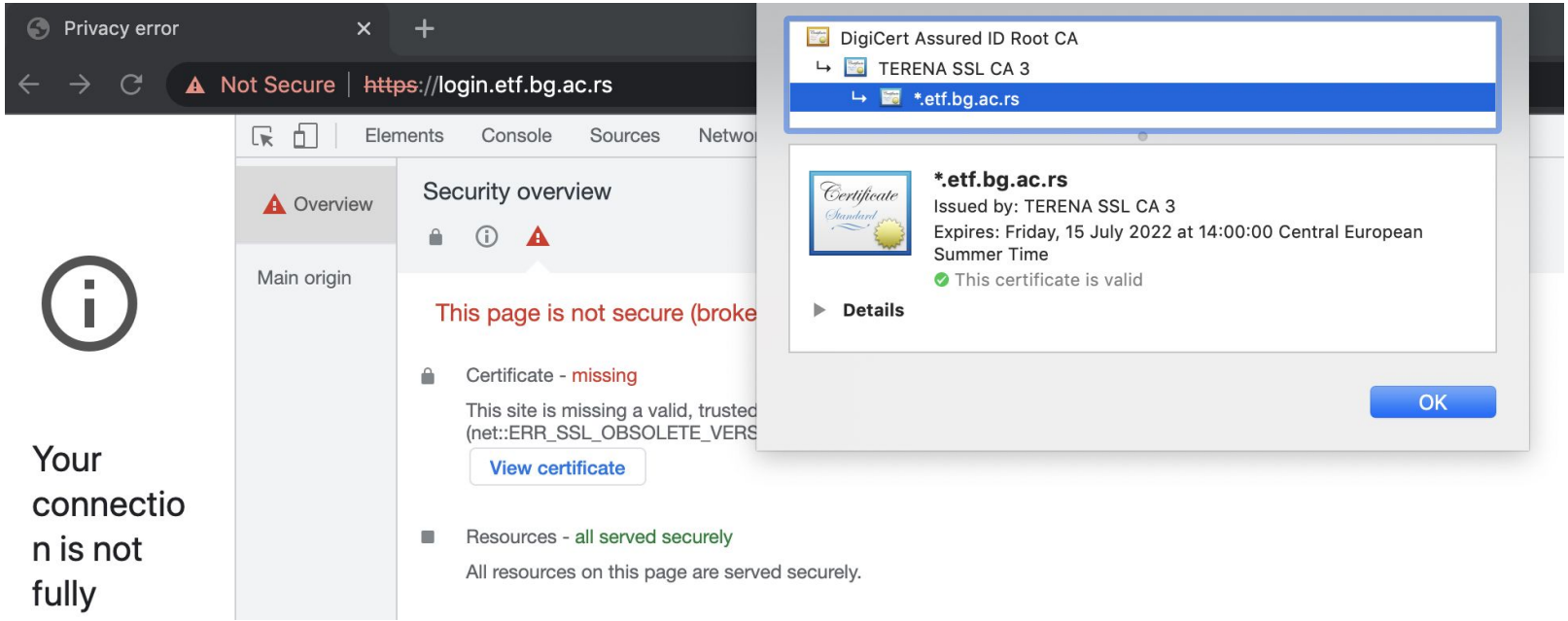
HTTPS, a ne piše “Secure”

3. Sertifikat koji je priložen nije validan za dati domen
   → primer: sertifikat je validan za `*.etf.bg.ac.rs`, ali ne i za `*.etf.rs`



HTTPS, a ne piše “Secure”

4. Komunikacija se vrši korišćenjem zastarelog SSL protokola
   → Uvek koristiti protokol TLS 1.3, on je najsigurniji!



HTTPS, piše “Secure”, a ne bi trebalo da bude

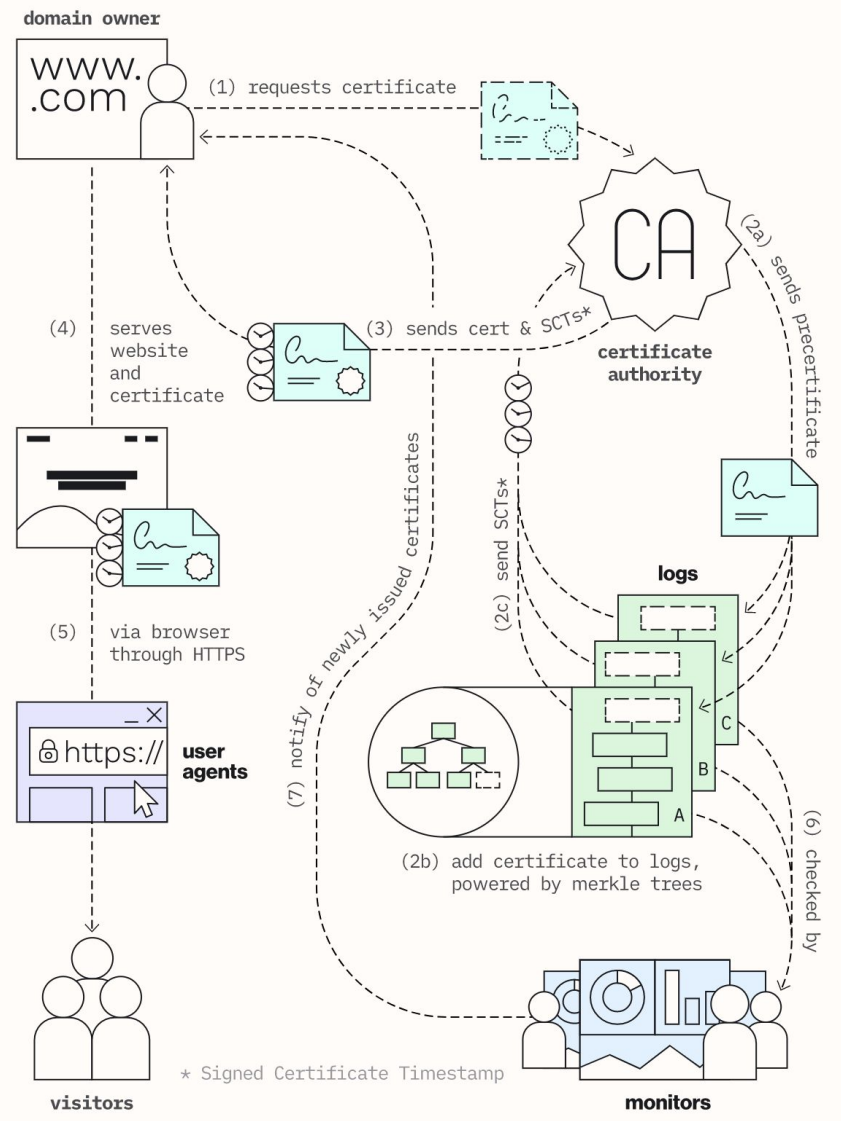
Da, ovo se takođe može desiti, i predstavlja *ogroman problem*. Na primer:

1. Privatni ključ sajta je ukraden
   → ljudi koji posećuju **taj sajt** možda zapravo komuniciraju sa prisluškivačem
2. Privatni ključ nekog CA je ukraden
   → ljudi koji posećuju **bilo koji sajt** možda komuniciraju sa prisluškivačem!
   → primer iz prošlosti: DigiNotar

Certificate Transparency

- Ako je privatni ključ nekog CA je ukraden, imamo ogroman problem!
- Treba nam sistem koji ovako nešto može brzo da detektuje, da bismo što pre prestali da verujemo tom CA
    - → Certificate Transparency je projekat koji baš ovo ima za cilj
    - → Više informacija: certificate.transparency.dev

Certificate Transparency



Hvala na pažnji!